

Security Overview

Summary of the administrative, technical and organisational security controls applied to the Jurion AI platform.

Document ID	JUR-LEG-006
Version	1.0
Effective date	2026-01-01
Last updated	2026-07-09
Category	security
Publisher	Jurion AI, jurion.uk

Subject to legal review

This document is provided for information only and remains draft until reviewed by a qualified solicitor. It does not constitute legal advice.

Jurion AI

info@jurion.uk
<https://jurion.uk>

Contents

1. Introduction	3
2. Encryption	4
3. Authentication	5
4. Multi-factor authentication	6
5. Role-based access control	7
6. Row-level security	8
7. Audit logs	9
8. AI governance	10
9. Incident response	11
10. Monitoring	12
11. Secure development	13
12. Continuous security reviews	14
13. Contact	15
14. General provisions and commercial protections	16
<i>Revision history</i>	18

1. Introduction

This document summarises the security controls applied to the Jurion AI platform. It is intended to support customer due diligence and procurement review.

This document does not claim any specific external certification. Where certifications are obtained they will be listed in this document and referenced in the Trust Centre.

2. Encryption

Data in transit between users and the Service is protected using Transport Layer Security (TLS) with modern cipher suites.

Managed database storage used by the Service is encrypted at rest using the encryption provided by the underlying cloud infrastructure.

Object storage buckets used by the Service are encrypted at rest using the encryption provided by the underlying cloud infrastructure.

3. Authentication

Authorised Users authenticate to the Service using email and password credentials, single sign-on where configured by the firm, or supported federated providers.

Password credentials are stored using industry-standard hashing algorithms. Session tokens are transmitted over TLS.

4. Multi-factor authentication

Multi-factor authentication is available for Authorised User accounts. Firms may require multi-factor authentication for users in privileged roles through the Firm Security Centre.

5. Role-based access control

The Service implements role-based access control. Roles are held in a dedicated authorisation table and evaluated by security-definer functions to prevent privilege escalation.

Firm administrators can assign, review and revoke roles through the Service.

6. Row-level security

Data in the Service is isolated at row level by policies enforced in the database layer. Policies restrict access to the firm and, where applicable, to the specific user or role authorised to view the record.

7. Audit logs

The Service records security-relevant events including authentication events, role changes, AI Feature usage and administrative actions.

Firm administrators can view firm-scoped events through the Firm Security Centre. Platform-level events are recorded for operational and security purposes.

8. AI governance

AI Features are subject to configurable governance controls held at firm level. Governance controls include enablement, rate limits, review requirements and logging. AI governance is described in more detail in the Jurion AI Responsible AI Statement.

9. Incident response

Jurion maintains an incident response process covering detection, triage, containment, recovery, customer communication and post-incident review. Further detail is set out in the Jurion AI Incident Response Policy.

10. Monitoring

The Service is monitored for availability, error rates and security-relevant events. Alerts are routed to the on-call engineering function for triage.

11. Secure development

Changes to the Service pass through source control review before deployment. Automated scanning is used to detect known vulnerable dependencies and common categories of security issue. Migrations to the database schema are versioned and reviewed.

12. Continuous security reviews

The security posture of the Service is reviewed on a continuous basis, and formal reviews are recorded in the internal Security Review Register. Findings are triaged, tracked and remediated according to their severity.

13. Contact

Security queries and responsible disclosure: security@jurion.uk.

14. General provisions and commercial protections

These general provisions apply to and form part of this document. Where a specific clause elsewhere in this document, in the Terms of Service or in the Data Processing Agreement addresses the same subject matter in greater detail, that more detailed clause prevails to the extent of any conflict.

14.1 AI limitations

Artificial intelligence features are assistive. Outputs are produced automatically and may contain errors, omissions, out-of-date information, inaccurate citations or content that is inappropriate for a specific matter. Jurion AI does not warrant that any AI output is accurate, complete, current or fit for any particular purpose and does not warrant that the Service is free from all errors or interruptions.

14.2 Human review requirement

Customer must ensure that a suitably qualified person reviews and approves any AI output before that output is relied on for legal advice, sent to a client, filed with a court or regulator, executed as a contract or used to make a decision that materially affects any person. Professional judgement of the reviewing individual remains authoritative.

14.3 Customer responsibility

Customer is responsible for its use of the Service, for the accuracy and lawfulness of the data it submits, for the actions of its authorised users and for compliance with applicable law and professional rules including where relevant the SRA Standards and Regulations. Customer must maintain appropriate matter management, supervision, conflict-checking and file-retention practices independently of the Service.

14.4 Acceptable use

Use of the Service is subject to the Jurion AI Acceptable Use Policy. Customer must not use the Service for unlawful purposes, to infringe the rights of any person, to attempt to circumvent the security of the Service, to submit content that is unlawful or that Customer does not have the right to submit, or in a way that materially degrades the Service for other customers.

14.5 Liability limits

Nothing in this document limits or excludes any liability that cannot be limited or excluded under applicable law, including liability for death or personal injury caused by negligence and for fraud. Subject to that, neither party is liable for indirect, incidental, consequential, special or exemplary damages, or for loss of profit, revenue, goodwill, anticipated savings, business opportunity or reputational loss, however arising.

Subject to the above, each party's total aggregate liability arising out of or in connection with this document in any twelve-month period will not exceed the fees paid by Customer to Jurion AI in that period. To the maximum extent permitted by law, the Service is provided "as is" and Jurion AI disclaims all warranties, whether express or implied, including any implied warranties of satisfactory quality, fitness for a particular purpose and non-infringement, other than those that cannot be excluded under applicable law.

14.6 Pilot status

Where the Service or a specific feature is provided on a pilot, beta, preview, evaluation or early-access basis, that Service or feature is provided "as is", may change or be withdrawn at any time and is not covered by the service-level commitments applicable to generally-available features. Pilot terms in the applicable order or the Pilot Programme Terms prevail over inconsistent provisions in this document.

14.7 Third-party services

The Service integrates with third-party services including cloud infrastructure, model providers, email providers, calendar providers and payment providers. Those third parties operate under their own terms and privacy notices. Jurion AI is not responsible for the availability, performance or acts and omissions

of third parties beyond its reasonable control, and Customer's use of any third-party service through the Service is subject to that third party's terms.

14.8 Data protection roles

Where Jurion AI processes personal data on behalf of Customer in connection with the Service, Customer is the controller and Jurion AI is the processor, and the Jurion AI Data Processing Agreement governs that processing. Where Jurion AI processes personal data as controller (for example account and billing data of authorised users and website analytics), the Jurion AI Privacy Policy governs that processing.

14.9 Service changes

Jurion AI may from time to time modify, add to or remove features of the Service in order to improve it, to reflect changes in third-party services, to reflect changes in law or regulatory guidance or to maintain security. Jurion AI will not make changes that materially reduce the overall functionality of the Service during a paid subscription term without giving reasonable prior notice.

14.10 Suspension rights

Jurion AI may suspend access to the Service or to specific authorised users, in whole or in part, where Jurion AI reasonably believes that continued access presents a security risk, that fees are materially overdue, that use of the Service is in material breach of this document or the Acceptable Use Policy, or that suspension is required by law or by a request from a competent authority. Where practicable Jurion AI will notify Customer before suspending access and will restore access as soon as the relevant circumstances have been resolved.

14.11 Security responsibilities

Jurion AI implements the technical and organisational security measures described in the Jurion AI Security Overview. Customer is responsible for configuring the Service in line with its own security requirements, for managing authorised user access including timely off-boarding, for enabling multi-factor authentication for its administrators, for protecting credentials and end-user devices, and for the security of any data that Customer chooses to export from the Service.

14.12 Draft status

This document remains draft and is subject to legal review until reviewed and approved by a qualified solicitor. It is provided for information only, does not constitute legal advice and should not be relied on as a final legal instrument until it has been so reviewed.

Revision history

Version	Date	Summary
1.0	2026-01-01	Initial published version.